BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

REPLY COMMENTS

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
Seven Parkway Center. Suite 755
Pittsburgh, PA 15220
(412) 922-8300

Thomas Cohen
John J. Heitmann
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
(202) 342-8518

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

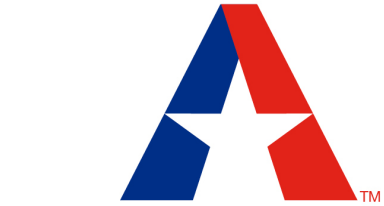
July 6, 2016

TABLE OF CONTENTS

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	

REPLY COMMENTS



The American Cable Association (ACA)[1] hereby submits its reply comments in response to the Notice of Proposed Rulemaking adopted by the Federal Communications Commission (Commission) in the above-referenced dockets.[2]

---

[1] ACA represents approximately 750 small and medium-sized cable operators, incumbent telephone companies, municipal utilities, and other local providers. In aggregate, these providers pass nearly 19 million homes and serve nearly 7 million homes. The vast majority of ACA members have fewer than 5,000 subscribers, and half have fewer than 1,000 subscribers. These small providers are characterized by a number of attributes that are relevant for the Commission to consider as it deliberates on adopting new and modified privacy and data security regulations for broadband Internet access service (BIAS) providers and whether to amend existing privacy and data security rules for voice and cable services.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (the NPRM or the Broadband Privacy NPRM).

I. INTRODUCTION AND SUMMARY

In this proceeding, the Commission proposes to diverge from the sensible and successful approach to privacy and data security that the FTC has used for decades in favor of an unprecedented and unduly prescriptive privacy regime that would do more harm than good for consumers, providers, and the Internet economy as a whole. The Commission should resist the siren song of various public interest commenters—whose proposals would needlessly increase costs and burdens for providers, particularly small ones, with little to no consumer benefit—and instead adopt a framework that is harmonized with the FTC's "unfair or deceptive acts or practices" standard and finds widespread support in the record.

In its initial comments, ACA challenged the Commission's authority to impose its proposed privacy and data security rules; described the burdens that the new rules would impose; and proposed alternatives that would ease the burdens placed on small providers while still achieving the Commission's goals of transparency, consumer choice, data security, and data breach notification. Specifically, ACA argued that the Commission does not have authority to adopt its proposed BIAS privacy and data security rules under Section 222 of the Communications Act, or under Section 201, 202, or 705 of the Act; Section 631 of the Cable Communications Policy Act; or Section 706 of the Telecommunications Act of 1996.[3]

[3] *See* Comments of the American Cable Association, WC Docket No. 16-106, at 9-22 (May 27, 2016) (ACA Comments). On June 14, 2016, the D.C. Circuit issued an opinion upholding the Commission's 2015 Open Internet Order reclassifying broadband Internet access service (BIAS) as a Title II telecommunications service. *See United States Telecom Ass'n v. FCC*, Slip Op. No. 15-1063. Petitioners in that case, including ACA, have the opportunity to appeal the D.C. Circuit's decision for *en banc* review or petition for certiorari to the Supreme Court. As such, ACA continues to assert that the Commission lacks authority to impose Title II common carrier regulations on BIAS, including the proposed privacy and data security rules.

ACA also asserted that the Commission's proposals would impose tremendous burdens on all providers, and these burdens would be specifically onerous for small providers. These burdens include, but are not limited to:

- development and implementation costs associated with data security controls, website policies, and customer approval tracking systems;
- personnel costs associated with dedicated privacy and data security staff;
- costs associated with all aspects of providing required notices and follow-up;
- attorney and consultant costs associated with regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits;
- third-party costs associated with modifying contracts and ensuring compliance for call centers, billing software, and others that interface with customer proprietary information; and
- opportunity costs associated with diverting scarce resources from innovation and infrastructure deployment to regulatory compliance.[4]

Rather than impose the unnecessary and heavy-handed rules proposed in the NPRM, ACA proposed that the Commission adopt rules consistent with the successful "unfair or deceptive acts or practices" standard of Section 5 of the FTC Act and as set forth in the Industry Proposal, which focuses on the Commission's core values of transparency, consumer choice, data security, and data breach notification, but would do so in a way that (1) would be consistent with privacy regulations for the rest of the Internet ecosystem, (2) would promote, rather than hinder, consumer choice and innovation, and (3) would not overburden small providers with micro-managerial, one-size-fits-all regulations.[5]

[4] *See* ACA Comments at 22-39.

[5] *See id.* at 39-42.

Alternatively, if the Commission pursues a prescriptive, *ex ante* privacy and data security framework as proposed in the NPRM, ACA proposed that the Commission adopt the following targeted exemptions for small providers:

- Exempt small providers from the specific "minimum" data security requirements that it sets forth in proposed Section 64.7005(a) and add "the size of the BIAS provider" to the factors that the Commission must consider when assessing the reasonableness of a BIAS provider's security program;

- Exempt small providers from the more onerous elements of its customer approval framework by grandfathering existing customer consents and exempting small providers from the requirement to obtain additional approval where they do not share sensitive personal information with third parties for marketing purposes;

- Exempt small providers from several elements of the Commission's proposed data breach notification rule (as applied to both voice services and BIAS) by exempting small providers from the specific notification deadlines in favor of an "as soon as reasonably practicable" standard; and

- Exempt small providers from any customer dashboard requirements that it adopts pursuant to its notice and choice regulations.[6]

These exemptions are consistent with existing privacy regimes and would directly address and partially reduce the significant burdens that the proposed privacy rules would have on small providers. ACA also called on the Commission to rationalize and streamline its proposed rules to ensure that the rules are not too burdensome for small BIAS providers by:

- developing, with industry and other stakeholders, standardized notices with safe harbor protection that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and developers;

- streamlining its proposed customer approval requirements to better align with consumer expectations and avoid disrupting existing customer relationships;

- adopting a general data security standard and work with industry to establish and update best practices rather than imposing prescriptive data security rules;

[6] *See id.* at 42-49.

- tailoring any data breach notification requirements to ease burdens on BIAS providers, including by adopting flexible deadlines for breach notification, limiting notifications to situations where consumer harm is reasonably likely, creating a one-stop-shop for breach reporting, and preempting state breach notification laws; and

- harmonizing its rules *within* Section 222, but not across statutory provisions including Section 631 of the Cable Act.[7]

ACA further proposed that the Commission extend the deadlines for small providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline (i.e., the date at which larger providers must comply with the rules), with a commitment to rule on a further rulemaking to determine whether to further extend the deadline and/or establish additional exemptions prior to the expiration of the general compliance deadline.

These reply comments proceed in several sections. Section II explains that proponents of the Commission's rules do not object to the Commission's consideration of specific relief for small providers, and highlights evidence in the record supporting ACA's contention that the proposed rules would impose significant burdens and costs on small providers. Section III highlights two additional issues not mentioned by ACA in its initial comments that also would be unduly burdensome for small providers. Specifically, ACA calls on the Commission to (1) reject any requirement to encrypt customer proprietary information or to impose specific encryption standards or practices, and (2) exempt business customers from the Commission's proposed rules. Section IV argues that there is widespread support, including from FTC staff, for adopting a flexible approach to privacy and data security consistent with the "unfair or deceptive acts or practices" framework that has traditionally governed privacy and data security in the Internet

[7] *See id.* at 49-58.

ecosystem, and that those who would impose a more stringent regime fail to appreciate the costs of such a proposal, particularly for small providers. Section V concludes.

II. PROPONENTS OF THE PROPOSED RULES DO NOT OBJECT TO RELIEF FOR SMALL PROVIDERS, AND THE RECORD FURTHER SUPPORTS ACA'S ARGUMENTS THAT THE PROPOSED RULES WOULD IMPOSE UNDUE BURDENS ON SMALL PROVIDERS

The NPRM asks numerous questions about the burden that its proposed rules would have for small providers, and seeks comment on whether—and if so, how—to provide relief to small providers.[8] In its initial comments, ACA asserted that the Commission's proposals would impose undue burdens on small providers, and called on the Commission, in the event that it rejects the Industry Proposal, to provide specific relief to small providers in the form of tailored exemptions, streamlined and rationalized rules, and extensions of generally applicable compliance deadlines.[9]

Notwithstanding the FCC's request for comment concerning small providers, proponents of the Commission's privacy and data security rules do not explicitly call for full application of the Commission's proposed rules to small provider or raise objections to specific relief for small providers.[10] Those few proponents that directly address the needs of small providers recognize

---

[8] *See, e.g.*, NPRM ¶¶ 89, 95, 101, 151, 177, 241.

[9] *See* ACA Comments at 22-37, 42-58.

[10] Instead, commenters in support of the NPRM ask the Commission to impose even more burdensome requirements (but do not suggest that these rules should apply with equal force to providers of all sizes). For example, some proponents call on the Commission to treat *all* customer proprietary information as sensitive information. *See* Comments of Public Knowledge, WC Docket No. 16-106, at 59 (May 27, 2016) (Public Knowledge Comments). Other proponents call on the Commission to require encryption of *all* customer proprietary information. *See* Comments of the National Consumers League, WC Docket No. 16-106, at 9 (May 27, 2016) (NCL Comments); Comments of New America's Open Technology Institute, WC Docket No. 16-106, at 41 (May 27, 2016) (OTI Comments). Proponents also urge the

that certain aspects of the rules would be too burdensome, and offer alternatives to reduce the burden on such providers. For example, the Electronic Frontier Foundation recognizes that any requirement to create a privacy dashboard "might prove to be a particularly heavy burden for small BIAS providers."[11] Access Now calls for small provider relief from the notice rules, arguing that "[s]mall providers should be allowed to resort to electronic notice delivery mechanism where reasonable to reduce costs."[12]

The vast majority of commenters that address small providers provide additional evidence to show the extent of the burden that the proposed rules, if adopted, would have on small providers, and call on the Commission to grant relief in line with ACA's proposals. Most notably, the U.S. Office of Advocacy for the Small Business Administration (SBA), an

---

Commission to require opt-in as a *default* for uses of customer proprietary information clearly within the customer's expectations. *See* Public Knowledge Comments at 31; Comments of the Center for Democracy and Technology, WC Docket No. 16-106, at 17-27 (May 27, 2016) (CDT Comments). These proposals, in addition to being completely out of step with prevailing laws and best practices, are oblivious to costs and second-order effects that would harm consumers and the Internet ecosystem as a whole. Requiring small providers to treat all customer proprietary information as sensitive, or to encrypt all customer proprietary information, would impose extreme costs and burdens, including but not limited to rewriting privacy and data security policies, implementing large-scale technical modifications to internal systems, hiring third-party consultants and outside counsel, and retraining personnel. Requiring opt-in consent across the board would similarly require enormous resources to make the necessary technical and administrative changes, would eviscerate existing validly obtained customer consents, and would curb existing and future investment in innovative service offerings. Any of these requirements would divert resources away from investment and innovation and toward unnecessary and overwhelming regulatory compliance obligations. The Commission should reject such a maximalist approach.

[11] *See* Comments of the Electronic Frontier Foundation, WC Docket No. 16-106, at 13-14 (May 27, 2016) (EFF Comments).

[12] *See* Comments of Access Now, WC Docket No. 16-106, at 6 (May 27, 2016) (Access Now Comments).

independent voice for small business within the federal government, with a Chief that is appointed by the President and confirmed by the U.S. Senate, argues "that the FCC's proposed rules will be disproportionately and significantly burdensome for small [BIAS] providers."[13] The SBA notes that "the FCC failed to comply with the [Regulatory Flexibility Act's] requirement to quantify or describe the economic impact that its proposed regulations might have on small entities," and "[t]he FCC has provided no estimate of the paperwork hours required to comply with the regulations."[14] Instead, "the FCC simply describes compliance requirements and seeks comment on compliance costs, without making any attempt to explain what kinds of costs small BIAS providers might incur in order to comply, and without any discussion of how those costs might be disproportionately burdensome for small entities."[15] For this reason, it is necessary that the Commission take heed of the concerns raised by ACA and others on these matters in this proceeding. ACA agrees with the SBA that "[b]ecause of resource constraints, complying with the proposed rules will be significantly more difficult for small BIAS providers," and that "[t]he record in this proceeding would support any effort by the FCC to mitigate the disproportionate compliance burden its proposal would have on small BIAS providers."[16] ACA supports SBA's call for the Commission to explore all alternatives that ACA and other small provider commenters raised in this proceeding, and further support SBA's proposal for "delayed

---

[13] Letter from Darryl L. DePriest, Chief Counsel for Advocacy, U.S. Small Business Administration Office of Advocacy, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 1-2 (May 27, 2016) (SBA Ex Parte).

[14] *See id.* at 2-3.

[15] *See id.*

[16] *See id.* at 3.

compliance schedules," as well as "exemptions for small BIAS providers wherever practicable."[17] Indeed, we agree that, in addition, "[g]iving small providers more time to comply with the FCC's rules will allow them to spread costs and manage their limited resources in a way that will minimize harm to their ability to serve customers."[18]

In addition, the record includes broad support for ACA's positions with respect to the NPRM's specific proposals on data security, customer approval, breach notification, notice, access, and third party oversight. In the following paragraphs, ACA addresses each of these issues in turn.

With respect to the Commission's proposed data security rules, ACA argued in its comments that the Commission's general data security standard would effectively impose a strict liability standard that would unduly burden small providers, and urged the Commission to modify its data security proposals to focus on reasonable data security measures—taking into account the size of the BIAS provider—rather than prescriptive requirements.[19] Many commenters agree.[20] CTA notes that the Commission's proposed strict liability data security standard "could be the death knell for smaller providers."[21] FTC staff likewise criticizes the

---

[17] *See id.*

[18] *See id.* at 4.

[19] *See* ACA Comments at 24 n.49, 44-45.

[20] *See* Comments of Consumer Technology Association F/K/A The Consumer Electronics Association, WC Docket No. 16-106, at 10 (May 27, 2016) (CTA Comments); Comments of the Rural Wireless Association, WC Docket No. 16-106, at 10 (May 27, 2016) (RWA Comments) (requesting that any data security rule "should apply a reasonability standard"); Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 27 (May 27, 2016) (FTC Staff Comments).

[21] *See* CTA Comments at 10.

Commission's strict liability standard, proposing instead that the Commission "modify[] the language to require BIAS providers to 'ensure the *reasonable* security, confidentiality, and integrity of all customer PI . . . .'"[22] Under FTC guidance, the reasonableness of a company's data security practices turns on "the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[23]

In its comments, ACA urged the Commission to avoid imposing specific data security requirements which would be unduly burdensome and would negatively impact the ability of small providers to adopt flexible and evolving data security controls.[24] The record provides further support for the conclusion that the Commission's proposed specific data security requirements rules would be unduly burdensome.[25] CCA aptly notes that "adding detailed and

---

[22] FTC Staff Comments at 27.

[23] Federal Trade Commission, Commission Statement Marking the FTC's 50th Data Security Settlement (January 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (March 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[24] *See* ACA Comments at 40-41, 53-57.

[25] *See* Comments of Competitive Carriers Association, WC Docket No. 16-106, at 40 (May 27, 2016) (CCA Comments) (challenging the requirement for regular risk management assessments as "overly burdensome," and raising concerns that "smaller providers would not be able to afford authentication and data security management tools" as the proposal would require.); Comments of NTCA – the Rural Broadband Association, WC Docket No. 16-106, at 58-66 (May 27, 2016) (NTCA Comments); RWA Comments at 10-12 (opposing specific qualifications for senior management officials and third party oversight); Comments of WTA-Advocates for Rural Broadband, WC Docket No. 16-106, at 23 (May 27, 2016) (WTA Comments) ("[R]equiring management-level hiring of specialized security experts in order to comply with new regulations would be particularly unreasonable for small, resource constrained RLECs due to their already

'robust' restrictions once again would force smaller carriers to yet again comply with arbitrary regulatory prescriptions at the expense of flexibility and efficiencies."[26] Based on the harm that the proposed rules would have on small providers, a number of commenters call on the Commission to adopt "principles rather than prescriptive rules" that "take size and resources into account" and are sensitive to the fact that small providers "may warrant a security approach different than that which would be most suitable to a larger firm."[27]

ACA also argued in its initial comments that that the Commission's data security proposals could inadvertently harm the ability of BIAS providers to engage in cybersecurity information sharing or to prioritize their threat responses, resulting in less security rather than more.[28] A number of commenters agree.[29] For example, CTIA argues that the "[t]he Commission should avoid creating legal uncertainty" with respect to information sharing "because any barrier to sharing information will create risk."[30] Similarly, Verizon notes that "[p]rescriptive data-security rules . . . could undermine the significant work that has gone into improving data security across the entire Internet ecosystem," which has resulted in "data-

---

small staff sizes and resources as compared to the salaries that full-time (or even part-time) experts can demand, as well as the lack or shortage of cybersecurity professionals in many rural areas.").

[26] *See* CCA Comments at 38.

[27] *See* Comments of the Wireless Internet Service Providers Association, WC Docket No. 16-106, at 25 (May 27, 2016) (WISPA Comments); NTCA Comments at 61; RWA Comments at 10; WTA Comments at 21.

[28] *See* ACA Comments at 32-33.

[29] *See* Comments of CTIA, WC Docket No. 16-106, at 141 (May 27, 2016); Comments of Verizon, WC Docket No. 16-106, at 66 (May 27, 2016) (Verizon Comments).

[30] *See* CTIA Comments at 141.

security improvements across the board and . . . the development of cybersecurity best practices, such as the NIST Cybersecurity Framework . . . ."[31] ACA agrees with Verizon that the Commission's proposed heavy-handed data security proposals "could jeopardize companies' ability and willingness to participate in such efforts in the future."[32]

With respect to the Commission's proposed customer approval framework, ACA explained that the Commission's proposal would unduly burden small providers by replacing a successful context-specific approach with one that would default to opt-in approval for most use cases and would require providers to obtain consent at a time that would not be in line with customer expectations.[33] Many commenters agree with this assessment. Cincinnati Bell supports the conclusion that the proposed customer approval framework would impede innovation, increase costs, and impair the ability to develop new uses and new revenue streams.[34] CCA notes that "[r]equiring changes to [customer approval] policies will require carriers to invest in additional legal work, pay their point of sale service providers to reprogram the customer contracts residing in the POS systems, pay third party website programmers to change the customer contracts residing on the website, and retrain sales and customer care representatives." [35] RWA explains that the customer approval framework would "disproportionately impact small BIAS providers, because these providers have only a few

---

[31] *See* Verizon Comments at 66.

[32] *See id.*

[33] *See* ACA Comments at 29-34.

[34] *See* Comments of Cincinnati Bell Telephone Company LLC, WC Docket No. 16-106, at 10 (May 27, 2016) (Cincinnati Bell Comments).

[35] *See* CCA Comments at 21.

thousand . . . subscribers . . . with which to absorb the costs of developing and implementing appropriate procedures."[36] The FTC staff criticizes the proposal to require BIAS providers to seek approval from customers after the point of sale but before the first use of data requiring consent,[37] and NTCA agrees that the approval timing would be "costly and burdensome."[38] As ACA did, several commenters call on the Commission to grandfather in existing consents for small providers.[39]

As for the Commission's proposed data breach notification rules, ACA argued in its comments that the burdens associated with that proposal would have an outsized impact on small providers.[40] Small provider commenters offer further support for ACA's argument. WTA notes that, for small rural providers, imposing a strict deadline is unnecessary "because small rural providers often live in and have strong ties to the communities they serve," incenting timely and complete notifications.[41] RWA explains that "[s]mall BIAS providers need additional time to determine the extent of any breach, as well as to consult with counsel as to the appropriate next steps."[42] FTC staff, while not specifically addressing small providers, argues that the breach notice timing "is too short and may not allow companies sufficient time to conduct an

---

[36] *See* RWA Comments at 9.

[37] *See* FTC Staff Comments at 24-25.

[38] *See* NTCA Comments at 52.

[39] *See, e.g.*, WISPA Comments at 31; RWA Comments at 9-10.

[40] *See* ACA Comments at 34-37.

[41] *See* WTA Comments at 13 ("Because small rural providers often live in and have strong ties to the communities they serve, they have strong incentive to provide their customers with complete and accurate information as soon as practicable.").

[42] *See* RWA Comments at 13.

investigation," which "could have a detrimental effect on consumers, who could get erroneous information about breaches."[43] FTC staff also notes that the Commission's overbroad data breach notification requirement would result in "companies that only collect data such as device identifiers or information held in cookies . . . collect[ing] *other* consumer information such as email addresses in order to provide consumers with breach notifications," and could lead to "overnotification."[44] Effectively requiring small companies to store more information about their consumers to comply with an overbroad regime would necessarily and unnecessarily increase the costs on small providers to the detriment, not benefit, of consumers.

Turning to the Commission's proposed notice rules, ACA argued in its comments that the Commission's proposal would be unduly burdensome and costly for small providers.[45] Commenters widely agree.[46] RWA notes that "[t]he internal information audits, project management and external legal and consultant service that will be necessary to comply with the Commission's [notice] proposals will require significant personnel and financial resources—resources that are already in short supply for small and rural wireless broadband carriers."[47] To alleviate burdens on providers and promote consumer awareness and comprehensibility, FTC

---

[43] *See* FTC Staff Comments at 32-33; *see also* WTA Comments at 13 ("providing . . . customers with incomplete or inaccurate information could leave the customer leery and could lead to a lack of trust in their provider.").

[44] *See* FTC Staff Comments at 31 (emphasis in original).

[45] *See* ACA Comments at 37-39.

[46] *See* CCA Comments at 17 ("Requiring competitive carriers to potentially adopt two different regimes for similar policies [i.e., Open Internet transparency and Section 222 transparency] will only create additional burdens, especially for small carriers, and will likely confuse customers."); NTCA Comments at 41 ("Requirements for printed or other forms of notice, and mandated periodic notices to consumer once past the sale, are unnecessary . . ."); RWA Comments at 6.

[47] *See id.* at 6.

staff argues that "the FCC should consider developing a standardized or 'model' notice" and should "provide a safe harbor, making clear that use of the model notice constitutes compliance with the rule's notice requirements."[48] ACA agrees that a model notice—coupled with a safe harbor—would be helpful in reducing the burdens for small providers, provided the notice is developed in a multi-stakeholder process that incorporates several small provider representatives in the process, and includes a dedicated working group to address the issues of small and medium-sized providers.[49]

Relatedly, in its comments, ACA opposed the Commission's proposals regarding access to customer proprietary information and related information and any requirement to develop and deploy a privacy dashboard.[50] With respect to access rights, commenters agree that an overbroad access requirement would be unduly burdensome for small providers. CCA argues that requiring broad access rights "would prove infeasible, particularly for small carriers with limited resources and personnel."[51] With respect to a dashboard requirement, small providers and their trade associations are universally critical.[52] As NTCA explained, "[f]or small providers[,] . . . the creation of such a comprehensive, interactive, individually-tailored interface would require significant resources aimed at customizing such a [dashboard] to reflect each consumer's

---

[48] *See* FTC Staff Comments at 13-14.

[49] *See* ACA Comments at 51.

[50] *See id.* at 26-27, 38-39, 46.

[51] *See* CCA Comments at 18.

[52] *See* Cincinnati Bell Comments at 15; NTCA Comments at 42; RWA Comments at 7; WTA Comments at 11-12.

status."[53] Even EFF, a public interest commenter, notes that "creating a privacy dashboard might prove to be a particularly heavy burden for small BIAS providers."[54] Moreover, a dashboard requirement would have minimal consumer benefit in part because the "dashboards are unlikely to be used by more than a small fraction of a provider's customers."[55]

With respect to requirements to exercise oversight over third parties through contractual terms or monitoring—issues on which the Commission sought comment in the NPRM—ACA explained in its comments that such requirements would be extremely burdensome—if not impossible—for small providers because they often lack the resources and bargaining power to impose or enforce them.[56] Commenters provide further support for ACA's argument. ACA agrees with CTIA's assertion that "[i]t is unrealistic for the Commission to expect ISPs, many of which are small- to medium-sized entities, to control the security practices of other entities," and "holding ISPs liable for the acts of third parties will have a disproportionate effect on small ISPs, who have to contract out more often and more extensively."[57] ACA further agrees with Cincinnati Bell that "[s]ervice [p]roviders should not be privacy police for their contractors,"[58] and CCA is correct that "small carriers do not have the litigation resources to enforce control they supposedly must exercise over consumer data."[59]

---

[53] *See* NTCA Comments at 42.

[54] *See* EFF Comments at 13.

[55] *See* Comments of Sprint Corporation, WC Docket No. 16-106, at 13-14 (May 27, 2016) (Sprint Comments).

[56] *See* ACA Comments at 27-28.

[57] *See* CTIA Comments at 151, 166.

[58] *See* Cincinnati Bell Comments at 14.

[59] *See* CCA Comments at 40.

III. THE COMMISSION SHOULD NOT IMPOSE AN ENCRYPTION MANDATE ON SMALL PROVIDERS, AND SHOULD PROVIDE A BROAD BUSINESS CUSTOMER EXEMPTION FROM ANY PRIVACY AND DATA SECURITY RULES IT ADOPTS

Commenters identify additional costs and burdens associated with several items that ACA did not address in its initial comments. The first is the Commission's question whether to require BIAS providers to encrypt all customer proprietary information or whether to impose specific encryption standards or practices. The second is the Commission's failure to incorporate a business customer exemption in its proposed rules. As explained below, ACA submits that a requirement to encrypt all customer proprietary information or to impose specific encryption standards or practices would be unduly burdensome and should not be adopted. Further, the Commission should establish a business customer exemption to provide small BIAS providers and their business customers with flexibility to negotiate their own privacy and data security terms, and should expand its existing business customer exemption to cover notice, approval, security, and breach notification

A. Substantial Evidence Shows That Mandating Encryption or Specific Encryption Standards or Practices Would Be Extremely Costly for Small Providers

In the NPRM, the Commission sought comment on whether to "require or encourage BIAS providers to use standard encryption when handling and storing personal information."[60] A few commenters call on the Commission to mandate encryption of customer information. For example, the Electronic Privacy Information Center (EPIC) asks the Commission to "require that service providers offer robust, end-to-end encryption for all consumers free of charge."[61]

---

[60] *See* NPRM ¶ 216.

[61] *See* Comments of the Electronic Privacy Information Center, WC Docket No. 16-106, at 23 (May 27, 2016) (EPIC Comments).

Similarly, OTI requests that the Commission "require encryption of customer data," arguing that "failing to use encryption to protect private information is unjust and unreasonable, and puts customers at unnecessary risk of data breaches."[62]

Many commenters oppose the idea of requiring BIAS providers to encrypt customer proprietary information. Access Now, which generally supports the NPRM, notes that in order to ensure that the Commission's rules "are implementable for service providers of any size[,] . . . the rules need not specifically require the use of encryption."[63] WTA rightly argues that "the Commission should "not require . . . that all CPI be encrypted when stored by ISPs due to the cost of encryption that may outweigh the benefit."[64] ACA agrees with WTA that an encryption requirement "would be unduly costly and burdensome to implement."[65] As CTA notes, requiring "an ISP to spend scarce resources on efforts to encrypt large swaths of non-sensitive data . . . could be the death knell for smaller ISPs."[66] Similarly, INCOMPAS opposes mandating specific encryption technologies or practices "especially given that there is no delineation in the NPRM between sensitive and non-sensitive data."[67] Moreover, as XO argues, requiring providers "to meet specific encryption requirements, and to perform ongoing maintenance

---

[62] *See* OTI Comments at 41.

[63] *See* Access Now Comments at 12.

[64] *See* WTA Comments at 20.

[65] *See id.* at 20-21.

[66] *See* CTA Comments at 10.

[67] *See* Comments of INCOMPAS, WC Docket No. 16-106, at 14 (May 27, 2016) (INCOMPAS Comments).

related to those changes, would impose a significant cost burden that carriers and their vendors are not equipped to meet at this time."[68]

ACA agrees that the Commission should not mandate encryption or specific encryption standards or practices, which would impose tremendous costs on small providers. For small providers that store customer proprietary information in-house, the technical cost of implementing encryption for all customer proprietary information across a variety of systems would be staggering. Moreover, for small providers that rely on third party vendors for billing and customer service functions, an encryption mandate could require small providers to renegotiate their contracts to ensure that data is encrypted, and, if the vendor refuses (e.g., because it would be uneconomical), to find a new vendor or move data in house, either of which would be time consuming and costly. Further, the cost of keeping up with changing encryption standards would impose ongoing costs on small providers to protect largely non-sensitive information.

Rather than mandate encryption, the Commission could exempt encrypted data from the definition of "breach," as ACA argued in its initial comments.[69] Alternatively, the Commission could exempt encrypted customer proprietary information from the definition of "customer proprietary information" altogether, as WTA argues.[70] These exemptions would create meaningful incentives for small providers to encrypt customer proprietary information without

[68] *See* Comments of XO Communications, LLC, WC Docket No. 16-106, at 14-15 (May 27, 2016) (XO Comments).

[69] *See* ACA Comments at 56 & n.101

[70] *See* WTA Comments at 20.

mandating certain encryption standards or practices that would be unachievable or unaffordable for many small providers.

B. Applying the Proposed Rules to Business Customer Relationships Would Unduly Burden Small Providers

In the NPRM, the Commission fails to address one of the most important elements of its existing CPNI rules: the business customer exemption. Under the existing voice CPNI rules, carriers are free to "bind themselves contractually to authentication regimes other than those adopted [in the rules] for services they provide to their business customers that have a dedicated account representative and contracts that specifically address the carrier's protection of CPNI."[71] The Commission reasoned that "the proprietary information of wireline and wireless business account customers already is subject to stringent safeguards, which are privately negotiated by contract."[72] The exemption applies to the Commission's authentication rules, but not to section 222 or the remainder of the Commission's CPNI rules.[73]

A number of commenters urge the Commission to exempt business customers from the specific BIAS privacy and data security rules (not limited to authentication). Verizon proposes that "[t]he Commission should allow telecommunications service providers to reach agreements with businesses regarding privacy terms other than those outlined in the Commission's rules, as

---

[71] *See In the matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services,* CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, ¶ 3 (Released April 2, 2007) (2007 CPNI Order).

[72] *See id.* ¶ 25.

[73] *See id.*

long as such terms are specifically addressed in the contract between the parties."[74] CTIA too urges "the Commission to create carve outs for enterprise and small and medium business (SMB) customers—as the voice CPNI rules currently do for business customers,"[75] and calls on the Commission to "exclude from any [approval] regime the uses and disclosures of information from enterprise and other business customers."[76]

XO, which does not provide BIAS, cites the business customer exemption in support of its argument against harmonizing the Commission's proposed rules for BIAS with the existing CPNI rules, which "would impose—without any basis or benefit—new obligations on business service providers[,] . . . would ignore important differences between consumers and business customers, would not advance the goals of respecting consumer privacy and protecting consumer data, and would impose significant, costly, and unnecessary burdens on carriers . . . ."[77] For these reasons, XO argues that the Commission should not apply its proposed data security rules,[78] its proposed expansive definition of "customer proprietary information,"[79] its proposed

[74] *See* Verizon Comments at 63.

[75] *See* CTIA Comments at 82.

[76] *See id.* at 118.

[77] *See* XO Comments at 3.

[78] *See id.* at 3-4.

[79] *See id.* at 4.

customer approval rules,[80] or its proposed breach notification rules[81] to providers serving business customers.[82]

ACA agrees with these commenters that the Commission should permit BIAS providers to agree to separate privacy and data security terms with their business customers where the provider and customer have a contract in place that specifically addresses privacy and security issues. First, imposing onerous privacy and data security rules for business customers is unnecessary. Business customers are more sophisticated than retail consumers, and often negotiate detailed privacy and data security terms into their service contracts. Second, imposing the rules proposed in the NPRM on business customers would harm small BIAS providers' relationships with their business customers. Because those business broadband contracts tend to include specific terms with respect to privacy and data security, any prescriptive rules that the Commission adopts is likely to undermine existing contractual terms, requiring renegotiation of service contracts at great expense and inconvenience to small providers and their customers.

Relatedly, ACA agrees with XO that the Commission should not apply heightened restrictions on providers serving business customers under the existing CPNI rules for the sake of "harmonization." Instead, the Commission should expand its existing business customer exemption beyond authentication to ensure that providers and business customers remain free to bargain for specific notice, approval, security, and breach notification terms that meet their unique business needs. In this way, the Commission can ensure a consistent framework for

[80] *See id.* at 5.

business customers under its privacy and data security rules that respects the sophistication and needs of those customers and their providers.

In sum, the Commission should ensure that any final rules include a general exemption from the privacy or data security rules for BIAS and telecommunications providers serving business customers where the parties have a service contract in place addressing privacy and data security issues.

IV. MANY COMMENTERS, INCLUDING THE FEDERAL TRADE COMMISSION STAFF, AGREE THAT A FLEXIBLE, UNIFORM FRAMEWORK FOR THE INTERNET ECOSYSTEM IS SUPERIOR TO THE COMMISSION'S HYPER-REGULATORY, BIAS-SPECIFIC PROPOSAL

In its comments, ACA argued that the Commission should adopt a flexible approach to privacy and data security consistent with the "unfair or deceptive acts or practices" standard of the FTC.[83] A wide variety of commenters supported this concept, and call on the Commission to adopt a flexible approach to privacy and data security consistent with that historically taken by the FTC and the rest of the Internet ecosystem, as set forth in the Industry Proposal.[84]

---

[83] *See* ACA Comments at 39-42.

[84] *See* Comments of AT&T Services, Inc., WC Docket No. 16-106, at 31 (May 27, 2016) (AT&T Comments) ("[T]he Commission should ensure that any rules it adopts preserve as much substantive consistency as possible with the FTC's longstanding regime--not only because that regime has defined the rules of the road for two decades, but also because it is a case study in regulatory success."); Comments of CenturyLink, WC Docket No. 16-106, at 4-5 (May 27, 2016) (CenturyLink Comments)("Rather than impose this unprecedented privacy regime, the Commission should adopt a regime based on the framework set forth by a coalition of industry associations (Industry Framework)."); Cincinnati Bell Comments at 11 ("The reclassification of BIAS as a Title II service removes the FTC's authority over that segment of the Internet industry, but provides no compelling reason to treat providers of BIAS differently than they were treated before reclassification, or differently than the thousands of Internet content providers that consumers continue to access which operate under the FTC regime."); CCA Comments at 2 ("CCA and other trade groups have put forth a proposal for the FCC to adopt an approach similar to the FTC's framework in a telecommunications environment."); CTIA Comments at 3 ("Consistent with the limits of its statutory authority, the Commission should adopt rules based

Commenters largely are aligned with ACA's rationale for maintaining a flexible framework modelled after the FTC's successful approach. Specifically, many commenters agree with ACA's position that the FTC's flexible approach is superior to the FCC's proposed more prescriptive, *ex ante* privacy framework.[85] Moreover, commenters support ACA's argument that the Commission fails to provide a well-reasoned rationale for diverging from the FTC's successful approach.[86] In addition, the record contains overwhelming evidence that the failure to harmonize the FCC and FTC approaches would lead to a fractured Internet ecosystem, which would undermine consumer expectations, stifle competition, and cripple innovation. Perhaps the best advocate for a harmonized privacy regime is the FTC staff, which describes the FCC's

---

on the FTC's deception and unfairness standard."); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 97 (May 27, 2016) (NCTA Comments)("The Commission should adopt a framework that replicates the FTC's successful approach to preserve uniformity of privacy obligations in the broadband ecosystem.").

[85] *See* CTA Comments at 4; CTIA Comments at 5-6; Comments of ITIF, WC Docket No. 16-106, at 10 (May 27, 2016) (ITIF Comments); Comments of the Internet Association, WC Docket No. 16-106, at 4 (May 27, 2016) (Internet Association Comments); Comments of the United States Telecom Association, WC Docket No. 16-106, at 3 (May 27, 2016) (USTelecom Comments).

[86] Cincinnati Bell Comments at 11 ("The reclassification of BIAS as a Title II service removes the FTC's authority over that segment of the Internet industry, but provides no compelling reason to treat providers of BIAS differently than they were treated before reclassification, or differently than the thousands of Internet content providers that consumers continue to access which operate under the FTC regime."); NCTA Comments at 30, 46 ("[T]he Commission's proposal departs dramatically from the FTC framework in several key respects without offering a reasoned explanation for these departures or for the onerous rules that result from them."); Internet Association Comments at 7 (arguing that there is "simply no need for the FCC to reinvent the privacy and security wheel for such services."); Comments of T-Mobile USA, Inc., WC Docket No. 16-106, at 11 (May 27, 2016) (T-Mobile Comments) ("The NPRM fails to identify a problem with BIAS provider practices that needs to be remedied, or to demonstrate that the existing privacy framework or the marketplace is not protecting consumers."); Verizon Comments at 32-33 ("The Commission does not explain why an approach similar to the FTC's privacy framework ... would not suffice to achieve its goals.").

proposal to impose heightened requirements on only BIAS providers (to the exclusion of other players that collect as much or more information from consumers) as "not optimal."[87] CenturyLink explains that "[f]orcing BIAS providers to comply with rigid rules while other providers—those with equal or greater access to consumer information—are permitted to continue offering services under the FTC's more flexible regime will . . . make it more difficult for BIAS providers to compete in the online marketplace."[88] Further, as AT&T argues, the Commission's approach would provide no meaningful benefits for consumers because edge providers "would still be subject to the same flexible FTC-style regime as before and would go on collecting and using all of the same information the rules would inefficiently restrict ISPs from using."[89]

Proponents of the Commission's decision to depart from the FTC's flexible framework advance several proposed justifications for their position, none of which are persuasive. First, some proponents of the NPRM's proposal argue that different treatment of BIAS providers is justified as a statutory matter, i.e., that the text and purpose of Section 222 requires different treatment.[90] However, nothing in Section 222 compels the Commission to adopt a framework as prescriptive and expansive as it does in the NPRM. Indeed, the Commission's proposal—which covers all "customer proprietary information" and imposes hyper-restrictive notice, customer approval, and data security requirements—is the product of its own overbroad and unlawful

---

87 *See* FTC Staff Comments at 8.

88 *See* CenturyLink Comments at 26.

89 *See* AT&T Comments at 50.

90 *See* Public Knowledge Comments at 4, 24.

reading of the statute.[91] Even if the statute did require the onerous provisions that the Commission seeks to adopt in this proceeding, the Commission retains authority to forbear from those provisions.

Second, opponents of a flexible framework argue that different treatment between ISPs and edge providers is justified for competitive reasons. Public Knowledge argues that the perceived lack of competition in the broadband market—as compared to the edge provider market—justifies more onerous rules.[92] And yet, the edge provider market is dominated by just a handful of players. The market for mobile operating systems—which ACA members' customers use to access the Internet over in-home Wi-Fi connections—is dominated by two players: Apple and Google.[93] The top ten mobile apps of 2015 are owned by just three companies: Apple, Google, and Facebook.[94] The market for Internet advertising—the chief concern of public interest advocates—is dominated by just two players: Google and Facebook.[95] In the broadband market, by contrast, a consumer often has the choice of several fixed and mobile BIAS providers, and may access the Internet through multiple BIAS providers over the

---

[91] *See* ACA Comments at 9-22 (arguing that the Commission lacks authority to impose its proposed rules).

[92] *See id.* at 24.

[93] *See* Benedict Evans, *New Questions in Mobile* (Dec. 3, 2014), http://ben-evans.com/benedictevans/2014/11/20/time-for-new-questions-in-mobile ("[T]he first phase of the platform wars is over: Apple and Google both won.").

[94] *See* Nielsen, *Tops of 2015: Digital* (Dec. 17, 2015), http://www.nielsen.com/us/en/insights/news/2015/tops-of-2015-digital.html.

[95] *See* Aleksandra Gjorgievska, *Google and Facebook Lead Digital Ad Industry to Revenue Record, Bloomberg* (Apr. 21, 2016), http://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record; USTelecom Comments at 15.

course of a single day (e.g., home fixed BIAS, mobile BIAS, a work connection, and public Wi-Fi).[96] Moreover, despite the fact that historically BIAS and edge providers have been subject to the same regime (Section 5 of the FTC Act), FTC enforcement history reveals a significantly higher number of privacy and data security enforcement actions against edge providers than ISPs.[97] These facts demonstrate that harsher treatment for ISPs on the basis of the competitive landscape is simply unwarranted.

Third, Public Knowledge argues that a flexible approach is improper because it would require deep-packet inspection to differentiate between sensitive and non-sensitive information.[98] Public Knowledge is mistaken. As an initial matter, Public Knowledge fails to distinguish between content traversing the network and information that a BIAS provider maintains about a customer, for example, in a customer relationship management system. Most of the information that small BIAS providers maintain about their customers—including information that traditionally has constituted CPNI—falls into the latter camp, and is readily separable into sensitive and non-sensitive categories without resorting to deep-packet inspection. Moreover, to

---

[96] *See* Peter Swire et al., Online Privacy and ISPs, 25, 121 (Feb. 29, 2016), *available at* http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

[97] *See* Federal Trade Commission, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network, Press Release (Mar. 30, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, Press Release (Nov. 29, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; Federal Trade Commission, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books, Press Release (Feb. 1, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

[98] *See* Public Knowledge Comments at 24-26.

the extent that Public Knowledge suggests that flexible, context-specific, and evolving privacy standards are "patently absurd," we respectfully submit that the FTC's long and successful history of privacy guidance and enforcement, coupled with ACA members' excellent track record in protecting their customers' information, suggest otherwise.

V. CONCLUSION

The record provides ample support for the conclusion that the FCC's proposed broadband privacy rules would impose tremendous costs and burdens on small providers with limited, if any, consumer benefit. The Commission should reject calls to adopt its proposed rules (or to make them even more burdensome and disruptive), and should instead adopt a flexible framework that respects the needs and means of small providers, as proposed in ACA's initial comments and herein.

Respectfully submitted,

By: Thomas Cohen

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
Seven Parkway Center
Suite 755
Pittsburgh, PA 15220
(412) 922-8300

Thomas Cohen
John J. Heitmann
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
(202) 342-8518

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

July 6, 2016